Chartered Institution of Railway Operators

Data Controller

Document Version 2.1

Data Audit: 9 March 2026

ICO REGISTRATION NO: ZA 281660

C O R P O R A T E
R E S P O N S I B I L I T Y:-

GEMMA BRICE
Data Protection Manager

DATA PROTECTION MANAGEMENT SYSTEM

Online Privacy Notice

CHARTERED INSTITUTION OF RAILWAY OPERATORS

Registered Member of the GDPR Check & Verify Register

www.gdprcheckandverify.com

1 COMPANY CONTACT DETAILS

1.1 Chartered Institution of Railway Operators 2nd Floor Beacon Building, Stafford Enterprise Park, Weston Road, Stafford ST18 0BF. hereinafter referred to as 'the Company', We, Us and Our.

1.2 Our email address is: admin@railwayoperators.co.uk

1.3 Our contact telephone number is: 03333 440523

1.4 We are a Data Controller under the provisions of the UK GDPR and the Data Protection Act 2018 and have registered with the UK Information Commissioners office:

ICO Registration Number: ZA 281660

2 Status of key personnel

2.1 We have designated **Ms Gemma Brice** as **Data Protection Manager** for the business.

2.2 We are not required to formally designate a Data Protection Officer (DPO) Because we are not engaged in any of the following activities:

(a) We are not a public authority.

(b) We are not an organisation that carries out the regular and systematic monitoring of individuals on a large scale.

(c) We are not an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

3 INTRODUCTION AND OVERVIEW

3.1 This Privacy Notice explains how we collect, use and protect personal data when you visit our website or contact us.

3.2 We are committed to protecting your personal information and complying with UK data protection law.

3.3 The Company is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

3.4 We have robust information security management systems in place to protect your personal data and have implemented appropriate technical and organisational security measures to protect it against any unauthorised or unlawful processing and against any accidental loss, destruction, or damage.

3.5 Pursuant to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) the Company must:

(a) use technical or organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

(b) implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Company's data

processing activities; and be able to demonstrate that it has used or implemented such measures and complied with the data protection principles.

(c) The Company maintains records of its own actions and our interactions with other Data Controllers and our Data Processors to ensure we can suitably demonstrate adherence to the data protection principles. Specifically, we ensure data is processed:

(i) Fairly, Lawfully and Transparently.

(ii) for limited purposes.

(iii) in a manner which is adequate, relevant and not excessive.

(iv) in a manner which is accurate and not kept for longer than necessary,

(v) in accordance with the prescribed rights.

(vi) in a manner which is secure and not transferred to countries outside the UK, without appropriate safeguards.

(vii) in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.6 This Online Privacy Notice is a precis of our written policies held at our business premises.

4 Scope of this Privacy Notice

4.1 This Privacy Notice applies to Personal Data we process when you visit or use our website. Further Privacy Policy statements and documents may apply offline and these are available, if relevant, on request.

4.2 We are committed to protecting your personal data privacy and, in accordance with relevant data protection laws, we uphold strict security procedures for the collection, storage, use and disclosure of your personal information.

4.3 We have described below the personal information we may gather about you, the purposes we will hold it for and the limited categories of people to whom we may disclose it.

5 What information do we collect and how do we use it?

5.1 During your visit to our site, we will only collect personal information that you choose to provide. If, for example, you contact us with an enquiry or request us to provide you with further information.

5.2 If you share other people's data with us, for example if you refer business to us on behalf of another, you will need to check you have lawful authority to do so. E.G. The other party has consented to you providing us with their information. In such a case you are responsible for ensuring the transmission to us of the information is lawful and we may ask you for documentary evidence of this.

6 Consequences of failing to provide Personal Data

6.1 In general if you fail or refuse to provide us with your Personal Data we will not be able to deal with your enquiry or do business with you. The following explains the consequences for each Lawful Basis of processing.

(i) Consent: It is your decision to provide your information by consent. We protect your data as described in this document but we cannot proceed with an enquiry without, for example your contact details to receive a reply.

(ii) Contract: We cannot contract with you for goods or services in business unless you provide us with, at least some of your details. We adhere to the principle of Data Minimisation and only collect enough data to complete the task at hand.

(iii) Legal Obligation: If we have a legal obligation to process your data, failure to provide the necessary information may have adverse consequences for you. If this is the case we will tell you.

(iv) Public Task: If we are required to process your personal data in the public interest or the exercise of official authority we will inform you. Failure to provide data under these circumstances will mean we cannot include you in the processing activity.

(v) Vital Interests**:** If data processing is required to protect the vital interests of a natural person then it is likely we will be in possession of the data before the need arises. If you have not provided us with your data this situation cannot apply to you.

(vi) Legitimate Interests: Where data processing occurs and has been deemed to be in our legitimate interests this will be based on a written assessment of need. There is usually no need for the data subject to provide their data for this purpose, although you do have the right to object to its use under certain circumstances but you usually must provide some identification data to make such an objection.

7 Using your data

7.1 We may use the information you provide us with in the following ways.

(i) To administer any account you have with us.

(ii) To perform our contractual obligations to you.

(iii) To respond to your queries and requests.

(iv) To communicate with you.

(v) To ensure that the content of our site is presented in the most effective manner.

(vi) To provide you with any information, products and/or services requested from us.

(vii) To provide you with helpful information about our products or services.

(viii) To make improvements to the service we provide you.

(ix) We also reserve the right to disclose your personal information where we are required to do so by law, such as to assist in any disputes, claims or

investigations relating to your account or contracts with us and to detect and prevent fraudulent transactions.

(x) E-mail correspondence with us via our website and email addresses accessible through or obtained from this site may be recorded and/or monitored.

8 How do we store and protect your data?

8.1 Data we receive and process is held by us in secure electronic devices and separate back up devices and servers.

8.2 Personal Data may also be held in encrypted 3rd party 'Cloud' Servers.

8.3 Further encrypted back ups of data may be held securely in offsite locations which are also subject to physical security at their location.

8.4 We will not sell, rent or otherwise disclose the personal information you provide to us through the site to third parties (other than as listed below) unless we are required to do so by law.

8.5 The Main Establishment for all of our Data Processing is the UK. We do not generally operate or transfer Personal Data outside of the United Kingdom.

8.6 Due to the operation of the Internet and other computer based applications Personal Data under our control may transit countries outside of the UK.

8.7 We will only transfer data outside the UK if adequate safeguards are in place in the destination country.

International Transfers of Data

8.8 Where Personal Data is transferred to a third country or an international organisation we will ensure that an adequacy decision or similar authority exists between the UK and the relevant country or area.

8.9 Where no adequacy decision exists and we rely on the provisions of Standard Contractual Clauses or Binding Corporate Rules evidence of the safeguards provided thereby will be available upon request.

8.10 In line with the DUAA's revised approach, We will assess whether the safeguards in place provide **protection that is not materially lower than the standard of protection in the UK**.

8.11 This assessment will be:

- Proportionate to the nature, volume, and sensitivity of the data;
- Focused on practical and foreseeable risks to individuals; and
- Documented as part of our accountability records.

8.12 Where risks are identified, We will implement additional technical, contractual, or organisational measures as appropriate.

9 Personal Data under our control.

9.1 The following is a chart of the personal data under our control.

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
Prospective and existing Clients providing their personal information either Online or Offline including Social Media, telephone and by written means to ourselves or third parties to request information regarding our available products and services	**Consent**	Identity Data Marketing Data Communications Data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Clients providing their information for the purposes of contracting with us for goods and services. We process this Personal Data to provide relevant advice, to manage and administer our business relationships and communicate with clients, their employees and representatives, to manage billing and payments and to keep records.	**Contract**	Identity Data Financial Data Transaction Data Marketing Data Communications Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.
Personal data provided because the Data Subject may be interested in working with us or learning more about working with us.	**Consent**	Identity Data	Time to consider request. Maximum of 12 months; or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
Online or Offline face to face meetings with people who provide their personal data to us for the purposes of later contact regarding products and services provided by us.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Suppliers of products and services to us who provide information of themselves or individuals who assist them to provide us with products and services on their behalf.	**Contract**	Identity data Transaction Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.
Personal Data of prospective customers provided by third parties for future contact by us regarding our products and services.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Suppliers of software who manage data via End User Service Agreements (EUSAs).	**Contract**	Identity Data Transaction Data Technical Data	Duration of Contract Plus Seven Years	Data is only shared with our authorised Data Processors.
Employees who provide their personal information for the purposes of working with us.	**Contract** **Legal Obligation** **Art.6 lawful basis** **Art.9 Condition (Employment)**	Special Category Data Identity Data Technical Data	Duration of Contract Plus Seven Years Any Other Legal Requirements	Data is shared with our Data Processors and our professional advisors including HMRC, IT, Accounts and Legal where necessary.

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
Information collected through the use of Website Cookies	**Consent**	Identity Data Marketing Data Communications Data Transaction Data Technical Data	Varies depending on the Consent given and type of Cookie based on information provided to users.	Data is only shared with our authorised Data Processors and professional advisers as necessary
Personal Data of individuals who make complaints under the DUAA 2025	**Legal Obligation**	Identity Data Technical Data	6 Years	Data is shared with our Data Processors our professional advisors and public bodies where necessary.
People identified via proprietary Video Conference software	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists, the client objects or within 3 months if recorded whichever occurs first	Data is only shared with our authorised Data Processors
Personal data collected at the time of purchasing or negotiating a contract with us using the 'Soft Opt in' exemption under the PECR Regs.	**Legitimate Interests**	Identity Data Marketing Data Communications Data	Until Legitimate Interest no longer exists, the client objects or the Data Subject Unsubscribes whichever occurs first	Data is only shared with our authorised Data Processors
People identified through our Dashcam Equipment	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists, the client objects or within 3 months if recorded whichever occurs first	Data is only shared with our authorised Data Processors

10 Types and Categories of Personal Data processed by the organisation may include

10.1 **Identity data:** name, username, title, date of birth. Contact data: billing and delivery address, email address, phone number.

10.2 **Financial data:** payment card details (processed by a third-party payment services provider and not stored by us).

10.3 **Transaction data:** details of products purchased, amounts, dates etc.

10.4 **Technical data:** IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform based on your Cookie preference choices.

10.5 **Profile data:** username and password, purchases or orders made by users.

10.6 **Usage data:** information about how users use our website, products and services.

10.7 **Marketing and communications data:** record of Website users preferences in receiving marketing from us about the products we sell.

11 Data sharing with others.

11.1 Below is a chart showing the organisations and individuals with whom we may share data.

Processor	Processor
Google AWS	**Glasgow University/ Keele University**
Microsoft Teams	**Teachus**
Zoom	**Stripe**
Social Media: Linkedin/WhatsApp FB/Tik Tok/Twitter/Snapchat/Instagram	**PlinkFizz Marketing**
Mailchimp	**Peninsula**
AI – Otter/ChatGPT/ CoPilot	**OFSTED/OFQUAL/ESFA**

12 Lawful bases for processing data

12.1 We hold and process your data by lawfully allowed means, these include:

(i) **Your Consent:** Consent is usually given by yourself when you contact us via this Website or personally when we discuss products or advice with you.

(ii) **Contractual obligations:** This occurs when you purchase products or services from us.

(iii) **Legal Obligation:** When the processing is necessary for us to comply with the Law.

(iv) **Vital Interests:** When the processing is necessary to protect someone's life.

(v) **Public Task:** When the processing is necessary for us to perform a task in the public interest or for an official function and the task or function has a clear basis in Law.

(vi) **Legitimate Interests:** When the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason

to protect the individual's personal data which overrides those legitimate interests.

(i) **N.B.** Legitimate Interests can only be used following the application of the prescribed three part Legitimate Interests Assessment Test and then only when a positive outcome is indicated by the conclusions of the test. All Legitimate Interests Assessment Tests will be documented, recorded and retained.

13 Policy Statement: Assessment of DUAA Recognised Legitimate Interests

Purpose

13.1 This policy statement records our assessment of the "recognised legitimate interests" introduced under the UK Data (Use and Access) Act 2025 (DUAA) and confirms the outcome of that assessment.

13.2 The DUAA amends the UK GDPR by introducing a limited set of **recognised legitimate interests** for which organisations may process personal data without undertaking a Legitimate Interests Assessment (LIA), provided the processing strictly falls within the categories defined in the legislation.

Assessment Outcome

13.3 We have reviewed the recognised legitimate interests set out in the DUAA, including (but not limited to):

(a) National security, public security, and defence

(b) Emergency response

(c) Safeguarding vulnerable individuals

(d) Crime prevention, detection, and investigation

(e) Other narrowly defined public interest purposes

Following this review, We have concluded that:

13.4 The nature of its activities does **not** involve processing personal data for any of the recognised legitimate interests defined under the DUAA; and

13.5 None of our current or planned processing operations fall within the scope of these recognised categories.

Lawful Basis for Processing

13.6 As a result, We do **not** rely on DUAA recognised legitimate interests as a lawful basis for processing personal data. Instead, all processing activities continue to rely on one or more of the established lawful bases under UK GDPR Article 6:

13.7 Where Legitimate interests is used, they will continue to be supported by a documented Legitimate Interests Assessment (where applicable)

Ongoing Review

13.8 This assessment will be kept under review and revisited if there are material changes to our business activities, the nature of its data processing, or further regulatory guidance is issued by the Information Commissioner's Office (ICO).

Accountability

13.9 This statement forms part of our accountability records under the UK GDPR and is available for inspection by relevant stakeholders and regulators upon request.

14 Your Personal Data Rights

14.1 Under the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. To exercise any of your rights contact our Data Manager using the details given above.

14.2 We protect the individual's rights provided by the UK GDPR and Data Protection Act 2018 as being the following:

(i) The right to be **informed** (Confirmation processing is taking place or not.)
(ii) The right of **access**
(iii) The right to **rectification**
(iv) The right to **erasure**
(v) The right to **restrict** processing
(vi) The right to data **portability**
(vii) The right to **object**
(viii) The right not to be subject to **automated decision making**, including profiling.

14.3 You have the right to request from us access to and rectification or erasure of your personal data; the right to restrict processing; the right to object to processing as well as in certain circumstances the right to data portability as below.

14.4 In the event that you provide your data directly to us for the purpose of a contract, or in circumstances where you have provided your data by consent, you have the right to be provided with your data in a structured, machine-readable format. This is known as Data Portability.

14.5 Following a request relating to Data Portability we will transmit the relevant personal data to the data subject or their nominated data controller where it is possible and technically feasible for us to do so.

14.6 Where you have provided your data voluntarily by Consent you have the right to withdraw your Consent at any time. However, withdrawal of Consent does not affect the lawfulness of any processing of your data based on your Consent prior to its withdrawal.

14.7 Where we need to process data for the purposes of entering into a Contract with you, if you fail to provide such data it may mean that we cannot establish legal relations between us and the contract may not be able to go ahead. We will inform you if this happens.

14.8 Automated decision making and profiling means making decisions without human intervention, usually with the use of a computer program or software. We may use automated decision making about you if it is necessary for entering into or performing a Contract with you or where you Consent to the actions.

14.9 Please note we will retain and use your personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. If we need to use your data for a reason it was not collected and you are not aware of this, we will inform you and in appropriate cases obtain your further consent to such use.

14.10 If we process data about you but we have not obtained the data personally from you, we must provide you with the information described in this Privacy Notice and some additional information.

14.11 The additional information will be provided to you at least by the time we contact you and in any event within the space of one month after we obtain it.

14.12 If the processing is based on Legitimate Interests, you are entitled to know what and whose Legitimate Interests they are.

14.13 You are entitled to know the purpose of the processing, whether we or someone else is processing it and the categories of Personal Data involved.

14.14 You are entitled to know the source of the information and whether the source is publicly accessible.

14.15 There are some exceptions to this additional information rule. If we obtain your Personal Data from a source other than yourself, the additional information rules will apply unless:-

(i) You already have the information regarding our processing; or

(ii) it would take a disproportionate effort or be impossible to provide you with it; or

(iii) you are already legally protected under separate provisions; or

(iv) we have a legal duty not to disclose it.

14.16 We use the lawful basis of Legitimate Interests for processing data in the following circumstances:

(i) When processing data using Video Conferencing software.

(ii) When processing data under the PECR Regulations for the ‘Soft opt in’.

(iii) When processing data using Dashcam equipment.

14.17 Our Specific Legitimate Interests are:

(a) Video Conferencing

(i) To facilitate efficient business video and telecommunications.

(ii) To protect the safety of our employees and participants on the call from unnecessary real world travelling.

(iii) To support our primary business objectives.

(b) Soft Opt in

(i) To promote efficient business marketing.

(ii) To increase sales of our products and services and support our primary business objectives.

(iii) To protect the personal data and the rights of our customers by using the correct procedures.

(iv) To support our primary business objectives.

(c) Dashcams

(i) To protect our Employees, business assets and our reputation.

(ii) To correctly record incidents which occur on the road.

(iii) To assist lawful authorities in the prevention and detection of crime.

15 Policy Statement: Automated Decision-Making and Profiling

Purpose

15.1 This policy statement documents our assessment of the use of automated decision-making and profiling and confirms the outcome of that assessment in accordance with the UK GDPR and the Data Protection Act 2018.

Definition

15.2 Under Article 22 of the UK GDPR, automated decision-making refers to decisions made solely by automated means, without meaningful human involvement, which produce legal effects concerning an individual or similarly significant effects. This includes certain forms of automated profiling.

Assessment Scope

15.3 We have assessed our processing activities across all business functions, including:

- Employment and workforce management
- Recruitment and selection
- Performance management and disciplinary processes
- Customer, client, and public-facing services
- Operational, financial, and administrative decision-making

Assessment Outcome

15.4 Following this assessment, We have concluded that:

- We does not carry out any decision-making that is based solely on automated processing;
- No automated processing produces legal effects or similarly significant effects on individuals;
- Any systems or tools used to support decision-making involve meaningful human review and discretion; and

- We do not engage in automated decision-making or profiling in relation to:
    - Staff members, workers, or job applicants; or
    - Members of the public, customers, or other external individuals.

15.5 Accordingly, Article 22 of the UK GDPR does not apply to our current processing activities.

Safeguards and Controls

15.6 Where technology is used to assist decision-making, We ensure that:

- Decisions are reviewed and approved by appropriately trained individuals;
- Individuals are not subject to decisions made solely by automated means; and
- Processing complies with the principles of lawfulness, fairness, transparency, and accountability.

Transparency

15.7 As We do not conduct automated decision-making within the meaning of the UK GDPR, we are not required to provide specific Article 22 disclosures in our privacy notices. Should this position change, transparency information will be updated accordingly.

Ongoing Review

15.8 This position will be kept under review and reassessed if there are material changes to:

- Business processes or services
- Use of artificial intelligence or automated tools
- Employment practices
- Applicable legislation or ICO guidance

16 Data Protection Complaints Policy

16.1 How to Make a Complaint

You can make a complaint to our Data Protection Manager by using our contact details provided above or by using the Online form on our Website.

16.2 Purpose of the Policy - This policy outlines how we handle complaints related to personal data under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025. It ensures individuals can raise concerns regarding the collection, processing, sharing, or access to their personal data and be assured of a fair, timely, and lawful response.

16.3 Scope of the Policy **-** This policy covers all personal data held in physical and electronic formats and applies to:

(i) Employees
(ii) Website Users
(iii) Third-party contractors
(iv) Any individual whose personal data is processed by us

16.4 Legal Framework - This policy is guided by the following UK legislation:

(i) UK General Data Protection Regulation (UK GDPR)
(ii) Data Protection Act 2018
(iii) Data (Use and Access) Act 2025
(iv) Privacy and Electronic Communications Regulations (PECR)

16.5 Grounds for Complaint - You may submit a complaint if you believe we:

(i) Processed your personal data unlawfully or without your consent or a lawful basis.
(ii) Denied your data subject rights, including:
(iii) Information/ Access
(iv) Rectification
(v) Erasure ("Right to be Forgotten")
(vi) Data portability
(vii) Restriction or objection to processing
(viii) Failed to provide transparency in data use or profiling.
(ix) Shared or accessed your data outside of approved legal parameters.
(x) Did not notify you of a data breach within the required timeframe.
(xi) Breached our obligations set out in the data legislation and Regulations.

16.5 Complaints Procedure - Once your complaint is received it will receive:

(i) Acknowledgement within **5 working days**
(ii) Initial assessment to determine validity and scope
(iii) Investigation within **30 calendar days** (complex matters may take longer, with notice)
(iv) A written response outlining:
    (i) Findings
    (ii) Any remedial actions taken
    (iii) Your rights and next steps

17.6 Remedies and Corrective Action - If we identify a failure or breach, we may take one or more of the following actions or others as appropriate:

(i) Amending or deleting incorrect data
(ii) Changing internal processes
(iii) Training or disciplining staff
(iv) Reporting incidents to the Information Commission (IC) where required
(v) Offering a formal apology (if applicable)

17.7 Escalation and Data Rights - If you are not satisfied with our handling of your complaint or the outcome, once we have investigated the complaint and replied, you may escalate the matter to the: Information Commission (IC). Their contact details are below.

Website: https://ico.org.uk/make-a-complaint/
Phone: 0303 123 1113
Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

17.8 Record Keeping - We maintain records of all complaints and outcomes for a minimum of 6 years, in line with our published Privacy Notice.

17 Artificial Intelligence

17.1 As an organisation we recognise both the importance of Artificial Intelligence in Data Protection and the need for controls within the technology.

17.2 We operate a Generative AI policy within the organisation and our Data Protection Manager is responsible for monitoring developments in this area.

18 Children's data

18.1 Our site is not directed at children and should not be accessed by them.

18.2 We will not knowingly collect information from persons under 13 years of age without their parent's or guardian's consent.

18.3 If a Parent or Guardian of a person under 13 years of age discovers their child has engaged with our Website without their consent, please inform us immediately using the contact email provided above.

18.4 We have considered the elements of the AADC (Children's code) in relation to our Online activity and concluded that we are not a relevant Information Society Service which is likely to be accessed by children.

18.5 There is nothing on our Website which could be damaging to children who view the pages or the pictures.

18.6 The products on our Website are only available and relevant to adults over the age of 18 years.

18.7 We protect the rights of the child in accordance with the UNCRC and the AADC by trading only with adults.

19 Third Party Websites

19.1 From time to time our site may contain links to and from the websites of our suppliers or other third party sites.

19.2 If you visit any of these sites you should confirm they have their own privacy policies and you should check these before submitting any personal data on their site. We cannot accept any responsibility or liability for the policies on any other Websites.

20 How to Access to Your Personal Data Held by us

20.1 When we respond to a Data Subject Access Request (DSAR), we take reasonable and proportionate steps to identify and provide the personal data requested, in accordance with the UK GDPR, the Data Protection Act 2018, and amendments introduced by the Data (Use and Access) Act (DUAA).

How We Search for Personal Data

20.2 We carry out searches that are reasonable and proportionate, taking into account:

20.3 The nature, scope, and context of the request

20.4 The volume and sensitivity of the personal data involved

20.5 The systems and records in which the data is likely to be held

20.6 The time and cost involved in carrying out the searches

20.7 We focus our searches using appropriate criteria, which may include:

20.8 Your name and known identifiers

20.9 Relevant dates or time periods

20.10 Specific business areas, systems, or types of correspondence

20.11 We are not required to carry out searches that would be disproportionate or excessive, including searches of unstructured data repositories where it would be unreasonable to do so.

20.12 If we need clarification to identify the personal data you are seeking, we may ask you to narrow or clarify your request. In these circumstances, the statutory response timeframe may be paused in line with applicable law.

How We Provide Personal Data

20.13 We will provide you with a copy of your personal data that falls within the scope of your request, subject to applicable exemptions and redactions.

20.14 In line with the DUAA, we may:

20.15 Provide your personal data in a reasonable and proportionate manner, rather than on a document-by-document basis; and

20.16 Exclude information that does not constitute your personal data or that falls outside the clarified scope of your request.

20.17 Where necessary, we may redact or withhold information to:

20.18 Protect the rights and freedoms of other individuals;

20.19 Preserve legal professional privilege; or

20.20 Comply with statutory exemptions under the Data Protection Act 2018.

Format of Our Response

20.21 We will normally provide your personal data in an electronic format unless you ask us to provide it in another way. We will ensure the information we provide is intelligible and accompanied by the supplementary information required under Article 15 of the UK GDPR.

Transparency and Your Rights

20.22 We document our search approach, the scope applied, and any limitations as part of our accountability obligations. If you are unhappy with our response, you have the right to raise concerns with us and to lodge a complaint with the Information Commissioner's Office (ICO).

20.23 Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

20.24 While it is not a requirement under UK GDPR that an individual must make a DSAR in writing, it is helpful for the Company if they do so. Individuals should therefore be encouraged to use the email address provided in this document.

20.25 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

- that is manifestly unfounded or excessive, e.g. repetitive; or
- for further copies of the same information.

Identifying the data subject

20.26 Before responding to a data subject access request, **the Data Protection Manager** will take reasonable steps to verify the identity of the person making the request.

20.27 We will not retain personal data, e.g. relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

20.28 If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm their identity.

20.29 Typically we will request a copy of the individual's driving licence or passport to enable us to establish their identity and signature (which should be compared to the signature on the data

subject access request and any signature we already hold for the individual). We may also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

20.30 If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request.

Refusing to respond to a request

20.31 We may refuse to act on a data subject access request where:

- even after requesting additional information, we are not in a position to identify the individual making the data subject access request;
- requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character.

20.32 If we intend to refuse to act on a data subject access request, we will inform the individual, within one month of receiving the individual's request:

- of the reason(s) why we are not taking action; and
- that they have the right to complain to the ICO and seek a judicial remedy.

Time limit for responding to a request

20.33 Once a data subject access request is received, the Company must provide the information requested without delay and at the latest within one month of receiving the request.

20.34 Therefore, a note of when request was received and when the time limit will end must be kept by **the Data Protection Manager and recorded in the data protection register**.

20.35 If a data subject access request is complex or the data subject has made numerous requests, the Company:

- may extend the period of compliance by a further two months; and
- must inform the individual of the extension within one month of the receipt of the request and explain why the extension is necessary.

Stop the Clock Procedure

20.36 In accordance with updated UK data protection legislation, We may pause ("stop the clock") the response timeframe where further information is reasonably required from the requester to:

- Clarify the scope of the request; or
- Identify the specific personal data being sought.

How the Stop the Clock Works

- The response period is paused from the date We request clarification;
- The clock resumes once the requested clarification is received;
- We will clearly inform the requester that the response timeframe has been paused and explain what information is needed.

20.37 The stop-the-clock procedure will only be used where clarification is genuinely necessary and not as a means to delay responding.

20.38 Please contact us if you believe that any personal data or information which we hold about you is incorrect or incomplete. Any information or data which is found to be incorrect will be corrected as soon as practicable.

20.39 Please contact us if you wish to have your personal data removed entirely from our systems. As soon as we are satisfied as to your identity and the data is not required to be kept for any other lawful reason or purpose it will be removed from our systems forthwith.

20.40 If you so wish, your Data will be provided to you electronically in a commonly used format such as email.

20.41 If you are unhappy with any of the responses given to you by us you may complain about us to the regulator at the Information Commissioners Office on 0303 123 1113 or through their website www.ico.org.uk.

21 Business Transfer or Sale

21.1 In the event our business, or part of it, is taken over, bought or merged with another business we may need to disclose any personal data we are holding about you to the other Company so they can continue to provide services to you in accordance with this Privacy Policy.

21.2 It may be necessary to transfer your data to a Company that is negotiating with us for the purchase of our business but only where it is necessary to evaluate the business purchase transaction.

21.3 In the case of a pre-sale transfer of personal data, the data would be kept safe during the negotiations and destroyed by the third party if the sale or merger did not go ahead.

22 Website Cookies

Purpose

22.1 This Cookie Policy explains how we use cookies and similar technologies on its website, in accordance with the UK Privacy and Electronic Communications Regulations (PECR), the UK GDPR, and amendments introduced by the Data (Use and Access) Act (DUAA).

What Are Cookies

22.2 Cookies are small text files that are placed on a user's device when they visit a website. They are widely used to make websites work efficiently, improve user experience, and provide information to website operators.

22.3 Cookies may be:

- **Session cookies**, which expire when the browser is closed; or
- **Persistent cookies**, which remain on the device for a set period or until deleted.

How We Use Cookies

22.4 We use cookies to:

- Ensure the website functions correctly
- Maintain security and prevent fraud
- Remember user preferences
- Understand how the website is used, in order to improve performance and content

22.5 Cookies may be set by us ("first-party cookies") or by third parties providing services on our behalf ("third-party cookies").

Cookies That Do Not Require Consent

22.6 Under UK law, as clarified by the DUAA, certain cookies may be used **without user consent** where they are strictly necessary for the website to function or for limited, low-risk purposes.These include cookies used:

- To enable core website functionality (e.g. page navigation, form submission)
- For security purposes, including fraud prevention and system integrity
- To remember user preferences essential to the service requested
- For **anonymous, low-risk statistical measurement** aimed at understanding website usage and performance, where:
    - Data is aggregated or anonymised;
    - It is not used to track users across websites; and
    - It does not significantly impact user privacy

These cookies are enabled by default and cannot be switched off, as the website would not function properly without them.

Cookies That Require Consent

22.7 Where cookies are used for purposes that are **not strictly necessary**, such as:

- Marketing or advertising
- Tracking users across websites
- Personalised content or profiling

We will obtain the user's **prior consent** before placing those cookies on their device.

22.8 Users will be presented with clear information and genuine choice through a cookie banner or preference tool.

Managing Cookie Preferences

22.9 Users can manage or withdraw their cookie preferences at any time by:

- Using the cookie settings tool available on the website; and/or

- Adjusting browser settings to block or delete cookies

Please note that blocking certain cookies may affect website functionality.

Third-Party Cookies

22.10 Some cookies may be set by third-party service providers, such as analytics or embedded content providers. These third parties are responsible for their own compliance with applicable data protection and e-privacy laws.

22.11 Where third-party cookies require consent, they will not be activated unless and until consent is provided.

Personal Data and Cookies

22.12 Where cookies involve the processing of personal data, that processing is carried out in accordance with our Privacy Policy, which explains:

- What personal data we collect
- The lawful bases relied upon
- How long data is retained
- Individuals' rights under UK data protection law

Changes to This Privacy Notice

22.13 This Privacy Notice may be updated from time to time to reflect changes in law, guidance from the Information Commissioner's Office (ICO), or changes to our use of cookies.

22.14 The latest version will always be available on our website.

22.15 There may be developments in how we use your data according to changes in the Law.

22.16 We reserve the right to make changes to this Data Protection and Privacy Policy at any time without notice and it is your responsibility to revisit this page from time to time to re-read this policy including any and each time you visit our website.

22.17 Any revised terms shall take effect as at the date of posting.

22.18 If you don't find your concern addressed here, feel free to contact us by e-mailing our Data Protection Manager at the contact details given above.

Contact Us

If you have questions about any of the Policies in this Privacy Notice, please contact us using the details above: